**Professional Summary**

* An information security professional specializing in cyber security – with expertise in conducting Vulnerability Assessments and Penetration Testing of Enterprise applications
* Worked for organizations in various verticals like – Media, Financial and Credit Risk Assessment.
* Knowledge of application security across the Software Development Life Cycle.
* Performed Threat Assessments and Incident Response activities across the SSDLC.
* Experience in application (Web & Mobile), Cloud Services, and network security.
* Expertise in performing secure code review (SAST) for different technologies like Java, Python etc.
* Experience in application and web services penetration testing (DAST). Using tools like Burp Suite, AppSpider and Postman.
* Experience in Android application penetration testing. Using tools like MobSF, ADB, Drozer, JD-GUI, Apktool, and Android Studio.
* Hands-on experience with Cloud services security assessments. Using tools like Prowler, Guard Duty.
* Ability to perform network vulnerability assessments using tools like Nessus, Nmap and Metasploit.
* Knowledge on binary analysis using toolset like BDBA (Black Duck Binary Analysis Tool).
* Exposure to open source security frameworks for vulnerability assessments namely Kali Linux.
* Good understanding of Buffer overflows, fuzzing, and ASLR bypassing.
* Experience in Malware analysis and reverse engineering

**Security Tools**

|  |  |
| --- | --- |
| Network Security Scanner | Nmap, Nessus Security Scanner, OpenVAS |
| Web Vulnerability Scanner | Checkmarx, Fortify Security center, Burp Suite Pro, and AppSpider |
| Mobile Pen testing tools | jadx, MobSF, Drozer, ApkTool, Ghidra, ADB, Andriod Studio, dotPeek, Hopper, & Burp Suite |
| Debugging Tools | Immunity Debugger, OllyDbg, and X64dbg  |
| Proxy Tools | Burp suite Pro, OWASP-ZAP |
| Exploit Tools | Metasploit Pro, msfpayload, SQLMap,& Mimikartz |
| Cloud services tools | Prowler, Guard Duty, AWS Config |

**Professional Experience**

**Intel Corp, CA** (ApplicationSecurity Enginee**r)** Oct 2018 – Present

Tools: Burp Suite Pro, Checkmarx, AppSpider, Drozer, MobSF, ADB, jdax, Andriod Studio, dotPeek, Hopper, X64 DBG, Splunk, GuardDuty, and APKTool etc.

* Performed Vulnerability Assessments on web applications, web services, and mobile applications
* Participate in security architecture reviews, provided defect walk-through to the application owners.
* Performed threat assessments/threat profiling to identify and track critical/high priority threats, risks, and attack vectors in the initial phases of Secure SDLC.
* Performing security assessments on next generation technologies like virtual reality and immersive media perform penetration testing of software and hardware components.
* Responsible for working with different stakeholders throughout the security development lifecycle
* Knowledge of log storage services like ELK stack(ES, LogStash, and Kibana), threat detection services like Amazon GuardDuty (AWS Cloud)
* Worked with Security Operations Center (SOC) on Splunk Correlation rules for incident response activities.
* Experience in microservice architecture & securing APIs across AWS cloud environment.
* Prepare final documentation/comprehensive report showcasing the security posture of the application with listed vulnerabilities, their details, business impacts and recommendations
* Analyze, review and audit code for security issues; work with development teams to remediate findings

**Equifax Inc, Alpharetta, GA (**Application Security Engineer/ Penetration Tester**)** Mar 2018 – Sep 2018

Tools: Burp Suite Pro Fortify on Demand

* Performed Threat Analysis for web applications
* Performed static code analysis on 10+ business applications.
* Performed web applications, web services penetration testing.
* Audited Fortify on Demand scan results and provided updated reports to the respective application teams.
* Provided security consulting to the application teams to fix the vulnerabilities.
* Worked with application teams to troubleshoot and fix build/ scan issues.
* Experience in securing CI/CD – Jenkins automation Pipelines.

**TMX Finance, Carrolton, TX (**Penetration Tester**)** Apr 2017 – Feb 2018

Tools: Nmap, OpenVAS, Wireshark, TCP Dump, SNMP-Check, Metasploit, Scuba Imperva, and Kali Linux (Open source distribution)

* Performed penetration testing and Vulnerability Assessment on Infrastructure (External and Internal) servers & Performed Database Security Assessment/Auditing.
* Participated in Architecture reviews and performed threat assessments.
* Identifying and exploiting network level vulnerabilities on open ports like SSH vulnerabilities, SSL certificate related vulnerabilities, RDP, FTP, SMTP, and SNMP Vulnerabilities etc.,
* Capturing and analyzing network traffic at all layers of the OSI model. Experience in using tools like wireshark & tcpdump.
* Performed network vulnerability assessments using tools to evaluate attack vectors, develop remediation plans, identify system vulnerabilities, and security procedures.
* Capturing Critical, High, Medium, and Low severity vulnerabilities in Servers and prioritizing them based on the criticality.

**Vsion Technologies (**Application Security Analyst**)** Aug 2016 – Mar 2017

Tools: Burp Suite, Nmap, Owasp ZAP & Kali Linux

* Performing Vulnerability Analysis/Penetration Testing
* Performing (Black box) testing for Websites
* Identify Threats and Vulnerabilities on particular Application
* Technical Report writing for findings with recommended solutions.

**Scrutiny Software, India (**Application Security Analyst**)** Jan 2013 – Dec 2014

Tools: Burp Suite, Owasp ZAP, sqlmap, and DirBuster etc.

* Responsible for conducting Vulnerability Analysis/Penetration Testing on Network Infrastructure and web applications
* Exhibited client facing skills and capability to articulate technical concepts to a variety of technical and non-technical audiences
* Identified issues on sessions management, Logging, Encryption, Privilege escalations etc.
* Performed daily vulnerability assessments, mitigation, threat assessment, and reporting activities to safeguard information assets and ensure protection has been put in place on the systems

**Relevant Coursework**

Principles of Secure SDLC, Software Security, Secure Architecture Reviews, Threat Modeling/Profiling, Static Code Analysis (SAST), Dynamic Assessments(DAST), Manual Penetration Testing, Vulnerability Assessments, Binary Analysis, and Incident Response.